Migrating Away From Compliance Quicksand

How a Modern Software Platform Can Resolve Your SOX Certification Issues

As a result of the corporate scandals at the turn of the century, U.S. lawmakers enacted the Sarbanes-Oxley Act (SOX) in 2002 as a mechanism designed to force U.S. corporations into certifying their financial information. After a few years scrambling to comply with SOX regulations, executives have come to realize that the impact of this regulatory framework on a company's IT systems is not only painfully obvious, but also far-reaching.

This white paper considers the latest developments regarding SOX compliance and explains how organizations can ensure ongoing certification by migrating their legacy finance applications to a modern IT platform.

By Juan Antonio Pastor

December 2006

While so far most organizations have been able to achieve Sarbanes-Oxley compliance every year, to do so they have had to deploy an unprecedented amount of resources and carry out exhaustive and tiresome auditing processes.

Most, if not all corporations in the United States and abroad depend on mission-critical software applications to keep track of their finances. The great majority of these applications are specific to the organizations themselves, designed to ease operations and give the company a competitive edge.

Without a doubt, the adequate functioning, control, and support of an organization's IT infrastructure is key when it comes to SOX compliance. To make the SOX compliance process more efficient, many companies have turned to specialized software designed specifically to help organizations meet the necessary regulations and controls by automating much of the required implementation.

The current reality that most organizations face, however, is that the applications and software infrastructure that they depend on to run their finances are patched-up, aging legacy systems that

face the risk of running unsupported. While SOX software can help a company meet certain requirements, the business value inherent in most legacy systems still remains under siege, partly because companies have focused on compliance issues and have put IT upgrade and modernization projects on the backburner, neglecting the importance of the latter on the first.

Organizations are beginning to realize that a modern, robust, and scalable IT system is the most ideal mechanism to enable the effective and timely compliance to SOX legislation regulations. Today, saying goodbye to the restraints of old IT systems by migrating to a modern software platform is both a real possibility and an urgent business obligation.

The Certification Headache Continues

Despite news reports in late November 2006 that federal regulators had eased restrictions somewhat, media outlets, technology experts, and audit consultants have all pointed out that these new guidelines are meant to facilitate an external auditor's job—not the corporation's. The regulatory burdens imposed by the law on IT departments remain heavy, especially if the IT infrastructure has not yet adapted to the Sarbanes lifecycle.

Fact is, the older the technology, the higher the risk of system failure, IT crashes, security violations, and prolonged downtimes. Companies with critical finance applications that are exposed to such potentially devastating threats cannot hope to achieve full SOX certification in the coming years and will be bogged down inescapably by the compliance process.

Even more pressing, legacy technology can conceivably result in prison time for high-level executives, and running unsupported under SOX legislation now has very real liability risks—something companies and organizations cannot afford to ignore.

Why Sarbanes-Oxley Strains IT

After the corporate scandals of the early 2000s, including those affecting Enron, Tyco, and WorldCom, shareholder trust in accounting and reporting practices declined considerably. As a result, the U.S. Congress passed the Sarbanes-Oxley Act of 2002, aimed at preventing financial misconduct and improving corporate governance practices.

While Sarbanes-Oxley is strictly focused on financial reporting and does not address technology, IT controls have both a direct and an indirect impact on the financial reporting process. As Network World points out in February 2005, “in its execution, SOX is all about IT.”

The software and systems that a company depends on for its daily business can spell the difference when it comes to keeping executives out of murky water. What this means—as has been noted repeatedly in the press—is that high management and board directors are now interested in and care more than ever about the IT infrastructure that the company is built upon.

Section 404 of Sarbanes-Oxley requires executives and auditors to confirm the effectiveness of internal controls for financial reporting, which implies that all software used by a company to carry out financial processes should be comprehensive, secure, clearly-defined, and well-maintained.

“When it [SOX] first came out, everybody was thinking about finances and the accuracy of year-end reports. But it starts to take on a life of its own,” argues Bernie Donnelly, Vice President of Quality Assurance and Control at the Philadelphia Stock Exchange, in a recent article. “Because when you ask that one question—‘Is this number accurate?’—then you have to ensure its accuracy. On the IT side, all these other things have to happen to answer that one question.”

Under SOX legislation, corporations—and more specifically, C-level executives—have to make sure IT is doing exactly what it was set up to do, especially when it relates to financial statements. “If I’m a CFO, I have to sign off on my company’s financial statements—and face criminal charges if my numbers are wrong,” comments Peter H. Knutson, Professor at the Wharton School of Business. “I rely heavily on those who manage the IT systems that produce those numbers.”

According to advisory firm AMR Research’s January 2005 Tech Trends study, 26 percent of 252 IT and business executives surveyed said compliance was the most important business driver of IT spending, taking precedence over other important initiatives like business-IT alignment, customer relationships, and other concerns.

The problem lies in the fact that, while executives recognize that software upgrade and business-IT alignment issues are critical for long-term SOX compliance, most have avoided taking action in this direction because of the scramble to meet first, second, third, and even fourth-year regulations. This has resulted in excessive yearly spending for most corporate IT departments.

Many corporate IT systems are facing obsolescence, but because they still satisfy business needs—at least to an acceptable measure—executives have not found it indispensable to upgrade this existing software infrastructure to guarantee the future survival of their company.

The decision to do so is perceived not as a strategic and rational investment but as a costly, complicated overhaul that should be put off for as long as possible. The move to postpone such a decision, however, can come at a price much higher than most executives and corporations can afford to pay.

Risks of Running Unsupported

In a July 2005 article discussing the issues related to unsupported software, Don Fowler points out that current government regulations “require your industry to stay current in your business enabling software,” and mentions that a failure in a company’s unsupported environment can lead to a serious violation of the Sarbanes-Oxley Act.

The consequences can range anywhere from hefty monetary fines and penalties, to jail time for high-level executives, to a devastating loss of reputation—any one of these unwanted outcomes will seriously aggravate an already-precarious situation by straining corporate resources and putting a business at real risk of going under.

Recently, the Institute of Internal Auditors linked the obligations under the Sarbanes-Oxley Act to a variety of specific recommended security practices, including the upgrade of operating systems and other software “to stay current with security patches and to ensure continuous vendor support for all software in use.” Failure to patch systems promptly or continued use of unsupported software can be viewed by courts as negligence.

While SOX does not provide for a private right of action in case individual clients are directly affected, companies can be fined for dragging their feet with their IT systems. Moreover, they can be held liable with respect to other parties if there is a perceived violation of a business-to-business contract regarding failure to meet established security practices or failure to achieve SOX compliance.

As Fowler explains, an unsupported environment can easily generate an operating deficiency—in SOX terms, this occurs when a control is not operating at it should—or there might be a technical

fault present in the system. If any one of these is directly involved with the administration of a company's finances and official support is no longer available, then the company is at risk of a serious SOX violation and C-level management must bear the legal consequences by default.

Essentially, to safeguard business integrity and avoid legal pitfalls, any company running unsupported software or that faces the risk of doing so has an obligation to migrate.

Migrate to Solid Ground

Corporations that do not count on a solid and scalable IT foundation are standing on a slippery slope. The continued and excessive spending in terms of time and money to meet compliance deadlines is unavoidable if a company's software infrastructure is increasingly patched-up, dependant on disparate technologies, and barely satisfying current business needs.

Also troubling, an inability or unwillingness to adapt and upgrade technologically can spur both speculation as well as unwanted scrutiny from shareholders, clients, and the federal government alike.

A comprehensive and well-maintained IT infrastructure built on a robust, modern platform and designed to maintain and protect an organization's business logic facilitates the auditing process immensely. For example, according to a September 2004 study conducted by Ernst & Young's Technology and Security Risk Services, the two issues presently responsible for the largest amount of audit exceptions are an inefficient segregation of duty controls and an excessive or improper user access to applications, servers, and data.

Thanks to technological breakthroughs, migrating a company's IT systems can now be done quickly and with minimal organizational disruption. By doing so, automatic processes can easily be put in place wherever needed, preventing these audit exceptions and making the auditor's job a whole lot easier—all this translates to reduced compliance costs.

Software modernization and integration provides the perfect opportunity to establish secure coding techniques to protect a company's finances from the get-go. According to Mark Salamasick, of the Institute of Internal Auditors, "an organization's defenses must include protection at Internet access points (i.e., routers and firewalls), in the applications and servers that process and store [financial]

data, and in each component of the infrastructure that may provide an access point for a threat to compromise security and provide unauthorized access to systems or data."

Through enhanced security that can automatically be put in place during the software modernization stage, it is possible to ensure that IT controls are updated and changed afterwards whenever necessary. In this way, a company can make changes in internal control and financial reporting processes transparently, removing vulnerabilities that might expose a system to viruses and other threats.

Moreover, migrating existing financial systems such as enterprise resource management applications to a modern platform can add specific functionalities capable of providing financial data in real time.

Streamline the IT Audit Trail

According to Alok Ajmera, Senior Manager in the World Class Finance Practice at BearingPoint, a global management and technology consulting firm in McLean, Virginia, under SOX legislation, a company's IT system must provide continuous, reliable monitoring of a company's financial information. "Executives need to be able to take a snapshot of that information and drill down further," he says. A migration project offers the possibility to adapt a company's critical finance applications to meet these specific requirements with little effort.

Through the use of effective internal and external portals, companies can also successfully account for changes that occur externally, such as changes by customers or business partners that impact its own financial positioning. Thus, complete and accurate financial information can be provided on demand.

According to a November 2006 study conducted by management software maker Approva, more than seven of 10 business executives say their firms lack a software solution that helps them conform to Sarbanes-Oxley's Section 404. Thirty-seven percent of the executives report that at least four-tenths of their I.T. controls are still done manually.

A software migration project allows a company to seamlessly integrate specialized SOX software with the rest of the IT infrastructure, enabling the creation of an integrated IT audit trail that

guarantees ongoing accountability and keeps executives in the clear, facilitating not only the external auditor's job but the corporate IT department's as well.

Integrating a company's IT infrastructure under a unified and modern platform also aids organizations with Section 802 of Sarbanes-Oxley, which includes a five-year record retention requirement. Due to the constant and rapid evolution in technology, legacy databases are at risk not because of data degradation but because of obsolete IT systems.

In a March 2004 article for Transform Magazine, Bruce Silver points out that current "software tools [designed] specifically for SOX compliance… lack a document repository that allows the work of control documentation, approval and testing to be distributed throughout the organization while maintaining access control," which is essential for long-term success with SOX compliance regulations.

Migrating existing records and creating adequate document repositories will ensure that improper document retention will not be a problem that will result in a fine or land an executive in jail.

Achieve Effective Corporate IT Governance

SOX has meshed finance and IT in a way that seems only to strengthen as this new regulatory framework matures and evolves. The tenets of SOX indicate that effective corporate IT governance must provide integrity, transparency, and accountability over a company's financial data.

Organizations must develop an ongoing compliance plan based on a robust, modern, and scalable IT platform to continue meeting SOX compliance regulations with ease for the years to come. This is essential when it comes to avoiding legal pitfalls and is also key as far as shareholder confidence is concerned, because any significant relief form regulatory compliance isn't happening any time soon.

Ironically, corporate myths seem to suggest that there are no concrete, viable, or cost-effective long-term solutions that effectively address specific IT business needs in terms of regulatory compliance. Most solutions focus on add-ons and specialized software that tend to complicate the already-complex IT landscape and limit corporate innovation.

While many SOX software packages can significantly ease compliance for many businesses and corporations, this might prove unwise in the long-run if all business applications do not already run on a modern platform.

With a well-planned, well-executed migration project, the consolidation of a corporation's IT infrastructure under a unified and robust operating platform can guarantee that clear, comprehensible, automated, and cost-effective financial processes will be put in place as required by SOX legislation, including the proper authorization of financial transactions, the safeguarding of assets against unauthorized or improper use, and the proper recording of transactions—not to mention the availability of continuous, ongoing vendor support.

Thanks to technological breakthroughs that enable the easy evolution to modern IT platforms, the possibility of true, sustainable, and effective corporate IT governance is now a reality. With a few years of SOX compliance experience under their belt, corporations now have an opportunity to focus their energy and resources on a strategic and long-term IT migration plan aimed at adopting a robust and scalable IT platform, not only for their critical finance applications, but also as the foundation for their entire IT infrastructure—a decision most organizations can no longer afford to postpone.

Related Links

"Compliance: Thinking Outside the Sarbox." Network World.
http://www.networkworld.com/research/2005/020705sox.html

"SarBox 404 Easing Soon? Don't Hold Your Breath." CIO Insight.
http://www.cioinsight.com/article2/0,1540,2061856,00.asp?kc=EWWHNEMNL113006EOAD

"To Run Unsupported – That is the Question."
http://www.mardon-y2k.com/To_Run_Unsupported.htm

"Look Beyond Records for SOX Compliance." Transform Magazine.
http://www.transformmag.com/showArticle.jhtml?articleID=18200846